IN THE SPECIFICATION:

Please insert after paragraph 3 at page 1, the following new paragraph:

WO 00/49505 A1 discloses a system for automatic connection to a network wherein a smart card contains the information specific to the user and/or the ISP to be accessed. The information contained on the smart card gets automatically retrieved when it is inserted into a smart card reader of the system and the information is used to gain the wanted access without having the inconvenience of the user having to search for the correct information.

Please replace paragraph 5 at page 1 continuing onto page 2 with the following rewritten paragraph:

According to the present invention, this object is solved by a method for securing an access to a predetermined area of a target server ~~as defined in independent claim 1~~, a method for starting a secure access to a predetermined area of a target server ~~as defined in independent claim 5~~, and a record carrier ~~as defined in independent claim 20~~. Preferred embodiments of the methods and record carrier according to the present invention are described ~~defined in the respective dependent claims~~. A computer program product ~~according to the present invention is defined in claim 18~~ and a computer readable storage means ~~is defined in claim 19~~ also are described.

Please replace paragraphs 1, 2, 3 and 4 at page 2 continuing onto page 3, with the following rewritten paragraphs:

The method for securing an access to a predetermined area of a target server according to the present invention comprises the step of providing an information file on a copy protected record carrier, which information file comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so

that the authentification server can initiate and confirm a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the authentification server and/or the project identifier, wherein said authentification server verifies whether or not a changing parameter of the computer, in particular a randomly generated number and/or a computer system time transmitted from said computer, was not already previously used and initiates a connection of said computer with said predetermined area of said target server in case of a positive verification .

Further, the method for starting a secure access to a predetermined area of a target server according to the present invention comprises the step of accessing of an information file on a copy protected record carrier, which information file comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so that the authentification server can initiate and confirm a connection between a computer on which said application is started and said predetermined area of said target server that is identified by the authentification server and/or the project identifier, wherein said autentification server verifies whether or not a changing parameter of the computer, in particular a randomly generated number and/or a company system time transmitted from said computer, was not already previously used and initiates a connection of said computer with said predetermined area of said target server in case of a positive verification.

Finally, the record carrier according to the present invention is copy protected and comprises an application and an information file, which information file comprises a project identifier and/or an address of an authentification server with which an application using said information file can communicate so that the authentification server can initiate and confirm a connection between a computer on which said application file is started and a predetermined area

of a target server that is identified by the authentification server and/or the project identifier, wherein said application transmits a changing parameter of the computer, in particular a randomly generated number and/or a computer system time to said authentification server so that said authentification server can verify whether or not the changing parameter of the computer was not already previously used and can initiate a connection of said computer with said predetermined area of said target server in case of a positive verification.

Therefore, according to the present invention the record carrier, e.g. a compact or digital versatile disc with audio and/or video information, comprises an information file, e.g. in a second session, and is copy protected by a generally known or future copy protection, e.g. the today used SecuROM copy protection, as described in the applicants European Patent EP 0 899 733 B1, which content is herewith included by reference. This guarantees that an application that accesses this file, or the information file as said application, can distinguish an original record carrier from a copy. With the data comprised in the information file the user can securely access the predetermined area on the target server that is preferably an internet server, e.g. the bonus material on a content server of the disc label. Since the data is provided in an executable file or accessible to an executable file, i.e. as an or within an application, that can access an automatic client/server authentification system preferably in a secure manner to grant access to certain target servers, e.g. websites, or areas, it can be secured that no key-codes, URLs etc. can be shared with others, since an access is only possible with the original record carrier in the disc drive. Further, the user experience/convenience is very good, since no complicated interaction, such as the typing of long serial codes, is necessary, but the access can be easily initiated, e.g. by a mouse-click. Preferably, the application opens the standard Web browser of the user/computer with the address of the authentification server and transmits at least the project identifier. The

security level is quite high, i.e. as high as the security level of the copy protection. Further, according to the present invention, said authentification server further verifies whether or not a changing parameter of the computer, in particular a randomly generated number and/or a computer system time transmitted from said computer, was not already previously used and initiates a connection of said computer with said predetermined area of said target server in case of a positive verification.

Please delete paragraph 1 at page 5.